**CYBER SECURITY STRATEGY ACTION PLAN**

**A NATIONAL CYBER PARTNERSHIP**

Goal: Governments, businesses and the research community together advance Australia’s cyber security.

|  |  |
| --- | --- |
| **Action** | **Outcome** |
| Deliver progress updates on the implementation of this Strategy | The Government evaluates its implementation progress and updates this Action Plan annually |
| Hold annual cyber security leaders’ meetings | The Prime Minister and business leaders set the strategic cyber security agenda and drive the Cyber Security Strategy’s implementation from the top-down  Business leaders and the Government are equipped with the information they need to make appropriate investment and business decisions on their cyber security, including a collective understanding of emerging cyber challenges |
| Streamline the Government’s cyber security governance and structures | Government responsibility for cyber security is well communicated and understood by stakeholders  The Prime Minister appoints a Minister Assisting the Prime Minister on cyber security  The Government’s cyber security operations are coordinated, efficient and align with strategic priorities  The Australian Cyber Security Centre is relocated to a facility that allows the Centre to grow and enables the Government and the private sector to work more effectively together |
| Sponsor research to better understand the cost of malicious cyber activity to the Australian economy | A better understanding of the economic impact of cyber compromises to the Australian economy is developed  Robust data is published that supports informed decision making on cyber security risk management and investment  Robust data is published that improves the ability of organisations to consider the effectiveness of their investment in cyber security |

**STRONG CYBER DEFENCES**

Goal: Australia’s networks and systems are hard to compromise and resilient to cyber attack.

|  |  |
| --- | --- |
| **Action** | **Outcome** |
| ***Detect, deter and respond*** | |
| In partnership with the private sector, establish a layered approach to cyber threat information sharing through:   * partnerships between businesses and the Government within the Australian Cyber Security Centre; * co-designed joint cyber threat sharing centres (initially as a pilot) in key capital cities; and * a co-designed online information sharing portal | Partnerships between the Australian Cyber Security Centre and the private sector are increased and proven valuable for both parties  An operating model for the joint cyber threat sharing centres is developed, successfully piloted and reviewed  Based on the outcomes of the pilot, a rollout of joint cyber threat sharing centres nationally improves co-location of businesses, the research community together with State, Territory and Government agencies and share:   * timely and actionable information on cyber security threats and risks; * knowledge about new/evolving actors and intrusion methods; and * expertise to solve problems and learn lessons from ‘near misses’ and compromises   Cyber security information is delivered to a wider range of organisations through the online information sharing portal |
| Increase the Computer Emergency Response Team (CERT) Australia’s capacity | [CERT Australia](https://www.cert.gov.au/)’s services are expanded for a wider group of businesses, with improved technical capability  CERT Australia increases its international partnerships, focusing on prevention and shutting down malicious cyber activity |
| Boost the Government’s capacity to fight cybercrime in the Australian Crime Commission | The [Australian Crime Commission](https://www.crimecommission.gov.au/) increases its capacity and capability to detect and analyse cybercrime |
| Boost the Government’s capacity to fight cybercrime in the Australian Federal Police | The [Australian Federal Police](http://www.afp.gov.au/) increases its capacity and capability to investigate cybercrime |
| Collaborate with Australian governments to ensure law enforcement officers receive the training they need to fight cybercrime across the nation | Skills needs for law enforcement officers, including specialist roles, to fight cybercrime are identified  A specialist training strategy is developed and implemented |
| Increase the Australian Signals Directorate’s capacity to identify new and emerging cyber threats to our security and improve intrusion analysis capabilities | The [Australian Signals Directorate](https://www.acsc.gov.au) increases its capacity and capability to identify cyber threats and develops responses to an increasingly complex digital environment  The [Australian Signals Directorate](https://www.acsc.gov.au) expands the number of cyber security services it offers to a wider range of organisations |
| Strengthen Defence’s cyber security capacity and capability, through initiatives in the 2016 Defence White Paper | Defence strengthens its cyber capabilities to protect itself and other critical Australian Government systems from malicious cyber intrusion and disruption  Defence enhances the resilience of networks, including networks used by deployed forces, and the capability of the Australian Cyber Security Centre and its cyber workforce, including new military and APS positions and training programs |
| Expand the nation’s cyber incident management arrangements and exercising program | The Government’s cyber incident management arrangements respond to the evolving cyber threat landscape  Australian governments understand how their respective cyber and incident response teams would operate together in a cyber crisis  The Government and private sector establish a program of joint cyber exercises  Australia works with international partners on developing policies for incident response as a confidence building measure |
| ***Raise the bar*** | |
| Co-design voluntary guidelines on good cyber security practice | The Government and private sector co-design and publish baseline guidance for Australian cyber security that provides a benchmark for good practice, informs cyber security insurance and meets corporate obligations  Australia’s good practice guidelines are an economic and security asset—they provide a commercial advantage and ensure cyber risks to critical services are risk assessed and managed  Australian businesses, small and large, have improved understanding of good cyber security practices  Governments, critical services and high risk sectors demonstrate good cyber security practices |
| Continue to regularly update the Australian Signals Directorate’s *Strategies to Mitigate Targeted Cyber Intrusions* | The *Strategies to Mitigate Cyber Intrusions* remain world leading publicly available advice on how to best protect against targeted malicious cyber activity |
| Co-design voluntary cyber security ‘health checks’ for ASX100 listed businesses | Executives and boards in the ASX100 better understand cyber security strengths and opportunities for their business  Decision makers in the ASX100 receive tailored information on the impact of cyber risks to their companies  Australia’s highest performing businesses lead a national effort towards best practice cyber security  Increased cyber resilience in Australia’s largest companies |
| Support the Council of Registered Ethical Security Testers (CREST) Australia New Zealand to expand its range of cyber security services | CREST Australia New Zealand grows its current pool of accredited companies to meet the demand of businesses accessing their services  CREST Australia New Zealand diversifies the services it accredits. Types of assessment might include penetration testing, vulnerability analysis and assessment against best practice standards |
| Support small businesses to have their cyber security tested by CREST Australia New Zealand accredited providers | Australian small businesses have access to accredited experts to assess their cyber security, helping them to take responsibility for the security of their own networks  Australian small businesses understand their potential cyber security vulnerabilities and where to find trusted cyber security advice  Australian small businesses are empowered with the knowledge they need to make considered cyber security investments to protect their business long term  Large and small businesses increase trust in the connections they have with each other |
| Improve Government agencies’ cyber security through a rolling program of independent assessments of agencies’ implementation of the Australian Signals Directorate’s *Strategies to Mitigate Targeted Cyber Intrusions* | Government agency cyber security practices are the exemplar for public and private sector organisations in Australia  Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability  Non Government information stored on Government networks is resilient to malicious cyber activity |
| Improve Government agencies’ cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings | Government agency cyber security practices are the exemplar for public and private sector organisations in Australia  Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability  Non Government information stored on Government networks is resilient to malicious cyber activity |
| Improve Government agencies’ cyber security through increasing the Australian Signals Directorate’s capacity to assess Government agencies’ vulnerability, provide technical security advice and investigate emerging technologies | Government agency cyber security practices are the exemplar for public and private sector organisations in Australia  Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability  Non Government information stored on Government networks is resilient to malicious cyber activity |
| Develop guidance for Government agencies to consistently manage supply chain security risks for ICT equipment and services | Government agencies have clear guidance on identifying and managing cyber security risks when procuring ICT equipment and services |

**GLOBAL RESPONSIBILITY AND INFLUENCE**

Goal: Australia actively promotes an open, free and secure cyberspace.

|  |  |
| --- | --- |
| **Action** | **Outcome** |
| Appoint a Cyber Ambassador | Australia has a coordinated, consistent and influential voice on international cyber issues |
| Publish an international engagement strategy on cyber security | Australia’s international engagement on cyber issues is prioritised and coordinated  Stakeholders understand Australia’s position on key cyber issues being debated on the world stage |
| Champion an open, free and secure Internet to enable all countries to generate growth and opportunity online | Australia actively participates in key international cyber fora to promote agreed peacetime norms of appropriate state behaviour in cyberspace |
| Partner internationally to shut down safe havens and prevent malicious cyber activity, with a particular focus on the Indo-Pacific region | Australia’s relationships with a broad range of international counterparts on operational cybercrime collaboration are strengthened  International efforts to prosecute cybercrime are enhanced |
| Build cyber capacity in the Indo-Pacific region and globally, including through public-private partnerships | Cyber capacity in the Indo-Pacific region, including through partnerships with businesses and the research community, is increased and contributes to improved cyber maturity |

**GROWTH AND INNOVATION**

Goal: Australian businesses grow and prosper through cyber security innovation.

|  |  |
| --- | --- |
| **Action** | **Outcome** |
| Establish a Cyber Security Growth Centre to bring together a national cyber security innovation network that pioneers cutting edge cyber security research and innovation, through the National Innovation and Science Agenda | Connections made between stakeholders, through the Growth Centre, deliver a multiplier effect on cyber security ideas and the number of challenges being responded to increases  More cyber security start-ups acquire capital to establish  More cyber security solutions are developed and commercialised  The number of cyber security businesses in Australia grows  More Australian cyber security products and services are exported  More international businesses invest in Australian cyber security research, innovation and solutions  All businesses benefit from cyber security solutions commercialised with Growth Centre support |
| Boost Data61’s capacity for cyber security research, support to commercialisation of cyber security solutions, improving cyber security skills and deepening connections with international partners, through the National Innovation and Science Agenda | Data61’s efforts on cyber security research and innovation have a multiplier effect on the activities within the industry-led Cyber Security Growth Centre's national cyber security innovation network  The number of students in cyber security PhD programs increase, through the support of Data61 scholarship programs  SINET is successfully established in Australia bringing together cyber innovators, buyers and investors, complementing activities of the Cyber Security Growth Centre​ |
| Work with business and the research community to better target cyber security research to Australia’s cyber security challenges | Australia’s cyber security R&D is robust, competitive and coordinated  Australia’s cyber security R&D explores current and emerging challenges for Australia’s national cyber security |
| Promote Australian cyber security products and services for development and export | The Australian public and private sectors mature their understanding of home-grown cyber security capabilities  The Government invests in developing Australian-based cyber security ideas  More international organisations invest in Australia and the Australian cyber security sector |

**A CYBER SMART NATION**

Goal: Australians have the cyber security skills and knowledge to thrive in the digital age.

|  |  |
| --- | --- |
| **Action** | **Outcome** |
| Partner with Australian governments, businesses, education providers and the research community in a national effort to develop cyber security skills:   * establish academic centres of cyber security excellence in universities; * to ensure qualifications in the ICT field provide cyber security skills; * introduce programs for all people at all levels in the workforce to improve their cyber security skills and knowledge, starting with those in executive-level positions; * continue to raise awareness in schools of the core skills needed for a career in cyber security; * understand and address the causes of low participation by women in cyber security careers; and * expand the Government’s annual *Cyber Security Challenge Australia* to a broader program of competitions and skills development. | The skills of university graduates and technical college students with cyber security qualifications are improved  The number of cyber security graduates increases  The number of children studying subjects at school that will equip them for careers in cyber security increases  More women and people with diverse backgrounds take up and change to a career in cyber security  People at all levels in the workforce, including those in executive-level positions, have the opportunity to improve their cyber security knowledge and skills by participating in competitions, short courses, executive training and other programs such as Masters degrees  Opportunities to participate in Australian cyber security competitions increases, including internationally |
| Bring together and grow public and private sector cyber security awareness programs to make the best use of combined resources | More people have improved knowledge of the real-world impacts of cyber risks and the way they affect our current and future prosperity |
| Work with other countries on cyber security awareness raising programs to deliver mutually beneficial outcomes | We achieve economies of scale through joined up awareness raising programs |